Discrete Mathematics 62 (1986) 85–98
North-Holland

ON THE NUMBER OF CYCLES OF SHORT LENGTH IN THE DE BRUIJN–GOOD GRAPH G_n

Zhe-xian WAN*, Rong-hua XIONG and Min-an YU
Institute of Systems Science, Academia Sinica, Beijing, China

Received 13 November 1984
Revised 20 November 1984

An algebraic approach to enumerate the number of cycles of short length in the de Bruijn–Good graph G_n is given and the following theorem is proved.

Theorem. *Let* $0 < m = k - n \leq \frac{1}{4}k + 1$, *then*

$$\beta(n, k) = \beta(k, k) - 2^{m-2}\phi_{k,m-1} - \sum_{l=1}^{m-2} \sum_{j=0}^{m-l-2} \sum_{2 \leq q < 1+(m-d_l-j)/l} \mu(q) 2^{d_l+e_j},$$

where $\phi_{k,m-1}$ *is defined to be the number of positive integers* $l \leq k$ *satisfying* $(k, l) \leq m-1$, $\mu(q)$ *is the Möbius function,* $d_l = (k, l)$, $e_j = 0$ *or* $j-1$ *according as* $j = 0$ *or* $j > 0$, *and* $\beta(k, k) = 1/k \sum_{d|k} \mu(d) 2^{k/d}$.

1. Introduction

An unsolved problem in the theory of shift register sequences is to enumerate the number of cycles of length k in the nth order binary de Bruijn–Good [1, 5] graph G_n, which we denote by $\beta(n, k)$. It is well known that this is just the number of cyclically distinct binary sequences of least period k which can be generated by non-singular n-stage feedback shift registers. By using combinatorial method, the authors of [2, 3] proved that for $n = k-1$, $k-2$ and $k-3$, $\beta(n, k) = \beta(k, k)$, $\beta(k, k) - \phi_{k,1}$ and $\beta(k, k) - 2\phi_{k,2} + 2$, respectively, where $\beta(k, k) = (1/k) \sum_{d|k} \mu(d) 2^{k/d}$ is the number of cyclically distinct sequences with period k and $\mu(d)$ is the Möbius function, and $\phi_{k,m}$ is defined to be the number of positive integers $l \leq k$ satisfying $(k, l) \leq m$. Bryant and Christensen [2] also proposed the following three conjectures:

Conjecture 1. *For* $k \geq 8$, $\beta(k-4, k) = \beta(k, k) - 4\phi_{k,3} - 2(k, 2) + 10$.

Conjecture 2. *For* $k \geq 11$, $\beta(k-5, k) = \beta(k, k) - 8\phi_{k,4} - (k, 3) + 19$.

Conjecture 3. *For* $k \geq 15$, $\beta(k-6, k) = \beta(k, k) - 16\phi_{k,5} - 4(k, 2) - 2(k, 3) + 48$.

In this paper, we give an algebraic approach to the enumeration of $\beta(n, k)$. With this method, we are able to prove an explicit formula of $\beta(n, k)$ when

* The first author thanks Professor O.T. O'Meara and the University of Notre Dame for their hospitality in the fall semester of 1984 during which this paper was revised.

$k - n \leqslant \frac{1}{4}k + 1$. And as an application of this formula, we prove the above three conjectures. In the meantime, another conjecture proposed by Christensen and Bryant [4] is also proved.

2. Basic concepts and the main results

We follow the notations in [2] and all the sequences are binary. We assume further that $n < k$.

Two sequences $\underline{a}$ and $\underline{b}$ are said to be cyclically equal if a cyclic shift of $\underline{a}$ equals $\underline{b}$, otherwise they are cyclically distant. A sequence of least period k is called an $[n, k]$ sequence if it has all k successive sets of n adjacent digits (called 'n windows') distinct, otherwise call it $\overline{[n, k]}$ sequence. We observe that $\beta(n, k)$ is just the number of cyclically disctinct $[n, k]$ sequences. If we denote by $\overline{\beta(n, k)}$ the number of cyclically distinct $\overline{[n, k]}$ sequences, then we obviously have

$$\beta(n, k) + \overline{\beta(n, k)} = \beta(k, k).$$

Let $\underline{a} = (a_0, a_1, \ldots, a_{k-1}, \ldots)$ be a sequence having least period k. By definition, $\underline{a}$ is an $\overline{[n, k]}$ sequence if there exist i and l, $0 \leqslant i < k$, $0 < l < k$, such that the $(i+1)$th n window $(a_i, a_{i+1}, \ldots, a_{i+n-1})$ equals the $(i+l+1)$th n window $(a_{i+l}, a_{i+l+1}, \ldots, a_{i+l+n-1})$. Let us call such a sequence an $\overline{[n, k]}_l$ sequence and denote their number by $\overline{\beta(n, k)}_l$ (considered cyclically).

In order to enumerate $\beta(n, k)$, we first enumerate $\overline{\beta(n, k)}_l$ for each l, $0 < l < k$, then $\overline{\beta(n, k)}$, and finally $\beta(n, k)$ by (1). The main results of this paper are as follows:

Theorem 1. (Christensen and Bryant's conjecture [4]). *Let* $0 < l < k$ *and* $(k, l) < m = k - n \leqslant \frac{1}{2}k$, *then* $\overline{\beta(n, k)}_l = 2^{m-1}$.

The case $(k, l) = 1$ was proved by Christensen and Bryant [4], and it is easy to show that $\overline{\beta(n, k)}_l = 0$ when $(k, l) \geqslant m$ (see [2] or the Remark in Section 3 of this paper).

Theorem 2. *Let* $0 < m = k - n \leqslant \frac{1}{4}k + 1$, *then*

$$\beta(n, k) = \beta(k, k) - 2^{m-2}\phi_{k,m-1} - \sum_{l=1}^{m-2} \sum_{j=0}^{m-l-2} \sum_{2 \leqslant q < 1 + (m-d_l-j)/l} \mu(q) 2^{d_l + e_j},$$

where $\phi_{k,m-1}$ *is defined to be the number of positive integers of* $l \leqslant k$ *satisfying* $(k, l) \leqslant m - 1$, $\mu(q)$ *is the Möbius function,* $d_l = (k, l)$ *and* $e_j = 0$ *or* $j - 1$ *according as* $j = 0$ *or* $j > 0$.

Theorem 3 (Bryant and Christensen's conjectures [2]).
For $k \geq 8$, $\beta(k-4, k) = \beta(k, k) - 4\phi_{k,3} - 2(k, 2) + 10$;
For $k \geq 11$, $\beta(k-5, k) = \beta(k, k) - 8\phi_{k,4} - (k, 3) + 19$;
For $k \geq 15$, $\beta(k-6, k) = \beta(k, k) - 16\phi_{k,5} - 4(k, 2) - 2(k, 3) + 48$.

3. The proof of Theorem 1

Let $F_2^k[x] = \{a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} \mid a_i \text{ in } F_2\}$. If $\underline{a} = (a_0, a_1, \ldots, a_{k-1}, \ldots)$ is a binary sequence with period k (not necessarily the least one), we associate it with a polynomial $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ in $F_2^k[x]$. Since this correspondence is clearly one to one, we will not distinguish between $\underline{a}$ (the sequence) and $a(x)$ (the polynomial of $\underline{a}$) and also call $a(x)$ a sequence. Now all the concepts concerning sequences $\underline{a}$ can be shifted to polynomials $a(x)$. For example, we say that $a(x)$ in $F_2^k[x]$ has (least) period p if its corresponding sequence $\underline{a}$ has (least) period p; $a(x)$ and $b(x)$ in $F_2^k[x]$ are cyclically equal (distinct) if their sequences $\underline{a}$ and $\underline{b}$ are cyclically equal (distinct); $a(x)$ is an $[n, k]$ ($\overline{[n, k]}, \overline{[n, k]}_l$) sequence if its sequence $\underline{a}$ is an $[n, k]$ ($\overline{[n, k]}, \overline{[n, k]}_l$) sequence.

The following lemma is immediate from definition.

Lemma 1. *Let* $a(x)$ *and* $b(x)$ *be in* $F_2^k[x]$. *We have*:

(i) $a(x)$ *and* $b(x)$ *are cyclically equal iff there exist* t, $0 \leq t < k$, *such that* $b(x) \equiv x^t a(x) \pmod{1 + x^k}$.

(ii) *The least period of* $a(x)$ *is the smallest integer* $p > 0$ *such that* $(1 + x^p)a(x) \equiv 0 \pmod{1 + x^k}$. *And* $p \mid k$.

Let $\underline{a} = (a_0, \ldots, a_{k-1}, \ldots)$ be a sequence having least period k and $a(x)$ its corresponding polynomial. If $\underline{a}$ is an $\overline{[n, k]}_l$ sequence, then it has two equal n windows. Without loss of generality, we may assume the two equal n windows to be the first $(a_0, \ldots, a_{n-1})$ and the $(l+1)$th $(a_l, \ldots, a_{l+n-1})$. Thus we have

$$(1 + x^{k-l})a(x) \equiv x^n g(x) \pmod{1 + x^k}), \tag{2}$$

where $g(x)$ is a polynomial of degree less than $k - n$. And it follows from Lemma 1(ii) that $g(x) \neq 0$.

Conversely, suppose $a(x)$ satisfies (2), where $g(x)$ is a non-zero polynomial of degree less than $k - n$ and $0 < l < k$. Direct verification shows that $\underline{a}$ has two equal n windows $(a_0, \ldots, a_{n-1})$ and $(a_l, \ldots, a_{l+n-1})$. If we make the additional assumption $0 < k - n \leq \frac{1}{2}k$, then we can prove that $a(x)$ has least period k. In fact, suppose $a(x)$ has least period p, $0 < p < k$. Then $p \mid k$, hence $0 < p \leq \frac{1}{2}k$. Multiplying both sides of (2) by $1 + x^p$ and using Lemma 1(ii), we obtain

$$(1 + x^p)g(x) \equiv 0 \pmod{1 + x^k}).$$

But, $\deg(1 + x^p)g(x) = p + \deg g(x) < k$, and this forces $(1 + x^p)g(x) = 0$, hence

$g(x)=0$, which contradicts to the assumption $g(x)\neq 0$. Thus, $a(x)$ is a sequence of least period k. Therefore, $a(x)$ is an $\overline{[n, k]_l}$ sequence. Hence we have proved

Lemma 2. *Let* $a(x)\in F_2^k[x]$.

(i) *If* $a(x)$ *is an* $\overline{[n, k]_l}$ *sequence, then there exists a non-zero polynomial* $g(x)$ *of degree* $<k-n$ *such that* (2) *holds.*

(ii) *Suppose* $a(x)$ *satisfies* (2), *where* $g(x)$ *is non-zero polynomial of degree* $<k-n$ *and* $0<k-n\leqslant \frac{1}{2}k$, *then* $a(x)$ *is an* $\overline{[n, k]_l}$ *sequence.*

In order to enumerate $\overline{\beta(n, k)_l}$, it is necessary to discuss for fixed l and $g(x)$, whether distinct solutions of (2) are cyclically distinct and for different $g(x)$ and $h(x)$ whether the solutions of (2) and the solutions of

$$(1+x^{k-l})b(x)\equiv x^n h(x)\ (\mathrm{mod}(1+x^k)) \tag{3}$$

are cyclically distinct. We have

Lemma 3. *Let* $0<k-n\leqslant \frac{1}{2}k$. *Then*

(i) *For fixed* l, $0<l<k$, *and non-zero polynomial* $g(x)$ *of degree* $<k-n$, *the distinct solutions of* (2) *are cyclically distinct*;

(ii) *Let* $h(x)$ *be another polynomial of degree* $<k-n$. *If* $h(x)=x^t g(x)$ (*or* $g(x)=x^t h(x)$), *then every solution of* (3) *is cyclically equal to a solution of* (2). *Conversely, if* $a(x)$ *and* $b(x)$ *are cyclically equal solutions of* (2) *and* (3) *respectively, then* $h(x)=x^t g(x)$ *or* $g(x)=x^t h(x)$, *where* $0\leqslant t\leqslant \frac{1}{2}k$.

Proof. (i) Let $a_1(x)$ and $a_2(x)$ be two distinct solutions of (2) which are cyclically equal. By definition we have

$$(1+x^{k-l})a_1(x)\equiv x^n g(x)\ (\mathrm{mod}(1+x^k)), \tag{4}$$

$$(1+x^{k-l})a_2(x)\equiv x^n g(x)\ (\mathrm{mod}(1+x^k)) \tag{5}$$

and there exists some t, $0\leqslant t\leqslant \frac{1}{2}k$, such that

$$a_1(x)\equiv x^t a_2(x)\ (\mathrm{mod}(1+x^k)), \tag{6}$$

or

$$a_2(x)\equiv x^t a_1(x)\ (\mathrm{mod}(1+x^k)). \tag{7}$$

Assume (7) holds. Multiplying by x^t on both sides of (4) and using (7) gives

$$(1+x^{k-l})a_2(x)\equiv x^n g(x)x^t\ (\mathrm{mod}\,(1+x^k)). \tag{8}$$

Comparing (5) and (8), we obtain

$$g(x)x^t\equiv g(x)\ (\mathrm{mod}(1+x^k)).$$

Since $\deg(g(x)x^t)<k$, we must have $g(x)x^t=g(x)$. Since $g(x)\neq 0$, $t=0$ and $a_1(x)=a_2(x)$. This completes the proof of (i).

(ii) Let $b(x)$ be a solution of (3) and let $a(x)\equiv x^{k-t}b(x)\ (\mathrm{mod}(1+x^k))$, where

$\deg a(x) < k$. Then $a(x)$ and $b(x)$ are cyclically equal, and

$$(1+x^{k-l})a(x) \equiv (1+x^{k-l})x^{k-t}b(x) \equiv x^n h(x)x^{k-t} \equiv x^n g(x) \pmod{1+x^k}).$$

Hence $a(x)$ is a solution of (2).

Conversely, if $a(x)$ and $b(x)$ are solutions of (2) and (3) respectively, and $a(x) \equiv x^t b(x) \pmod{1+x^k})$ for some t, $0 < t < k$. Then we have (as in the proof of (i)) $g(x) \equiv x^t h(x) \pmod{1+x^k})$, which implies that $g(x) = x^t h(x)$ (if $0 \leqslant t < \frac{1}{2}k$) or $h(x) = x^{k-t} g(x)$ (if $k > t \geqslant \frac{1}{2}k$). Thus we have proved (ii). □

By the above lemmas, for fixed l, $0 < l < k$, to enumerate $\overline{\beta(n, k)_l}$, it is sufficient to enumerate, for all polynomials $g(x)$ of degree less than $k-n$ with $g(0) = 1$, the number of solutions of (2). We need the following lemma, which is a simple result from algebra.

Lemma 4. *Let $0 < l < k$ and $(k, l) = d$. Let $g(x)$ be a polynomial of degree less than $k-n$. Then (2) has a solution iff $1+x^d$ divides $g(x)$. Furthermore, if (2) has a solution, it necessarily has 2^d solutions.*

Remark. We see that $1+x^d$ divides $g(x)$ implies $d \leqslant \deg g(x) < k-n$, hence (2) has no solution when $d = (k, l) \geqslant k-n$. Therefore, $\overline{\beta(n, k)_l} = 0$ if $(k, l) \geqslant k-n$. Thus the assumption of $(k, l) < k-n$ in Theorem 1 is natural.

We can now give the proof of Theorem 1.

Proof of Theorem 1. Write $(k, l) = d$ and $k-n = m$ for simplicity. Let $g(x)$ be a polynomial of degree $< m$ and $g(0) = 1$. In order that (2) has solutions, we must have $1+x^d$ divides $g(x)$. Thus we can write $g(x) = (1+x^d)g_1(x)$, where $g_1(x)$ is of degree $< m-d$ and $g_1(0) = 1$. The number of choice of $g_1(x)$ is 2^{m-d-1}. For each choice of $g_1(x)$, by Lemma 4, there are 2^d solutions of (2) and by Lemma 3(i), these 2^d solutions are cyclically distinct. And by Lemma 3(ii), the solutions of (2) for different choices of $g_1(x)$ are also cyclically distinct. Therefore

$$\overline{\beta(n, k)_l} = 2^{m-d-1} \cdot 2^d = 2^{m-1}.$$

This proves Theorem 1. □

4. The proof of Theorem 2

We prove in Theorem 1 that $\overline{\beta(n, k)_l} = 2^{m-1}$, where $m = k-n$. But $\overline{\beta(n, k)}$ is not a simple summation of $\overline{\beta(n, k)_l}$, where l runs from 1 to $k-1$. In fact, a binary periodic sequence $\underline{a}$ of least period k may be an $\overline{[n, k]_l}$ sequence and an $\overline{[n, k]_{l'}}$ sequence with $0 < l, l' < k$ and $l \neq l'$. For instance, let $a(x) \in F_2^k[x]$ be a solution of (2) and let $b(x) \equiv x^{k-l} a(x) \pmod{1+x^k})$, where $\deg b(x) < k$. Then $b(x)$

is cyclically equal to $a(x)$ and it is easily verified that $(1+x^l)b(x) \equiv x^n g(x) \pmod{1+x^k}$. Hence, for each $\overline{[n, k]}_l$ sequence $a(x)$, there exists an $\overline{[n, k]}_{k-l}$ sequence $b(x)$ such that $a(x)$ and $b(x)$ are cyclically equal, and therefore $a(x)$ is also an $\overline{[n, k]}_{k-l}$ sequence. Thus, an $\overline{[n, k]}$ sequence is necessarily an $\overline{[n, k]}_l$ sequence for some l, $0 < l \leq \frac{1}{2}k$. But $\overline{\beta(n, k)}$ is also not a simple summation of $\overline{\beta(n, k)}_l$, where l runs from 1 to $[\frac{1}{2}k]$. For example, $\{110100\ldots\}$ is a $\overline{[2, 6]}_2$ sequence as well as a $\overline{[2, 6]}_3$ sequence.

From now on, we assume $0 < m = k - n \leq \frac{1}{4}k + 1$. Note that in this case, if $(k, l) < m$, then $l \neq \frac{1}{2}k$ (since $l = \frac{1}{2}k$ would imply $(k, l) = \frac{1}{2}k \leq m - 1 \leq \frac{1}{4}k$, which is a contradiction).

Let

$$G(l, g) = \{a(x) \in F_2^k[x] \mid (1+x^l)a(x) \equiv x^n g(x) \pmod{1+x^k})\}$$

and

$$\mathcal{S} = \{G(l, g) \mid 0 < l < \tfrac{1}{2}k, \deg g(x) < m, g(0) = 1 \text{ and } 1 + x^{(k,l)} \text{ divides } g(x)\}.$$

It follows from Lemma 2 and Lemma 3 and the above discussion that $\bigcup_{G(l,g)\in\mathcal{S}} G(l, g)$ contains all the $\overline{[n, k]}$ sequences (considered cyclically) and that every sequence in $\bigcup_{G(l,g)\in\mathcal{S}} G(l, g)$ is an $\overline{[n, k]}$ sequence. But a given $\overline{[n, k]}$ sequence may appear in several $G(l, g)$'s. At first, we have

Lemma 5. $\sum_{G(l,g)\in\mathcal{S}} |G(l, g)| = 2^{m-2}\phi_{k,m-1}$, *where* $\phi_{k,m-1}$ *is the number of integers* $l \leq k$ *satisfying* $(k, l) \leq m - 1$.

Proof. Since $(k, l) = (k, k - l)$, the number of integers $l \leq \frac{1}{2}k$ with $(k, l) \leq m - 1$ is equal to $\frac{1}{2}\phi_{k,m-1}$. Hence by Theorem 1

$$\sum_{G(l,g)\in\mathcal{S}} |G(l, g)| = \tfrac{1}{2}\phi_{k,m-1} \cdot 2^{m-1} = 2^{m-2}\phi_{k,m-1}. \quad \square$$

To compute $\overline{\beta(n, k)}$, we have to exclude the number of repetitions from $2^{m-2}\phi_{k,m-1}$. The following lemma is crucial.

Lemma 6. *Let* $G(l_i, g_i) \in \mathcal{S}$ *and* $a_i(x) \in G(l_i, g_i)$, $i = 1, 2$. *If* $a_1(x)$ *and* $a_2(x)$ *are cyclically equal, then* $a_1(x) = a_2(x)$. *In this case,* $G(l_1, g_1) \cap G(l_2, g_2) = G(u, g)$, *where* $u = (l_1, l_2)$ *and*

$$g(x) = \frac{1+x^u}{1+x^{l_1}} g_1(x) = \frac{1+x^u}{1+x^{l_2}} g_2(x).$$

Proof. Since $a_1(x)$ and $a_2(x)$ are cyclically equal, $a_1(x)x^t \equiv a_2(x) \pmod{1+x^k}$ for some t. We may assume $0 < t < \frac{1}{2}k$. Since $a_i(x) \in G(l_i, g_i)$, $i = 1, 2$, we have by

definition

$$(1+x^{l_1})a_1(x) \equiv x^n g_1(x) \ (\mathrm{mod}(1+x^k)), \tag{9}$$

$$(1+x^{l_2})a_2(x) \equiv x^n g_2(x) \ (\mathrm{mod}(1+x^k)). \tag{10}$$

Multiplying (9) by $(1+x^{l_2})x^t/(1+x)$ and (10) by $(1+x^{l_1})/(1+x)$, we obtain

$$\frac{1+x^{l_2}}{1+x} x^t g_1(x) \equiv \frac{1+x^{l_1}}{1+x} g_2(x) \ (\mathrm{mod}(1+x^k)). \tag{11}$$

Since $1+x$ divides $g_i(x)$ $(i=1, 2)$, we can write $g_i(x) = (1+x)h_i(x)$ $(i=1, 2)$ and (11) becomes

$$(1+x^{l_2})x^t h_1(x) \equiv (1+x^{l_1})h_2(x) \ (\mathrm{mod}(1+x^k)), \tag{12}$$

where $\deg h_i(x) \leqslant m-2$.

If $l_2 + t + \deg h_1(x) \geqslant k$, then $l_2 \geqslant k - (t + \deg h_1(x)) \geqslant k - (\frac{1}{2}k + \frac{1}{4}k - 1) = \frac{1}{4}k + 1 > \deg h_1(x)$. It follows that x^{t+l_2} occurs in $(1+x^{l_2})x^t h_1(x) \ (\mathrm{mod}(1+x^k)) = (1+x^{l_1})h_2(x)$. Hence $\deg(h_2(x)) + l_1 \geqslant t + l_2 \geqslant k - \deg h_1(x) \geqslant \frac{3}{4}k + 1$. But on the other hand, $\deg(h_2(x)) + l_1 < \frac{1}{4}k + \frac{1}{2}k = \frac{3}{4}k$, which is impossible. This shows that we must have $l_2 + t + \deg h_1(x) < k$. Hence we obtain from (12) that

$$(1+x^{l_2})x^t h_1(x) = (1+x^{l_1})h_2(x). \tag{13}$$

Since $h_2(0) = 1$, this forces $t = 0$, and so $a_1(x) = a_2(x)$.

Next let $u = (l_1, l_2)$ and $a(x) = a_1(x) = a_2(x)$ be a common solution of (9) and (10). Since $t = 0$, (13) implies

$$\frac{1+x^{l_2}}{1+x^u} g_1(x) = \frac{1+x^{l_1}}{1+x^u} g_2(x).$$

Since $((1+x^{l_1})/(1+x^u), (1+x^{l_2})/(1+x^u)) = 1$, $(1+x^{l_1})/(1+x^u)$ divides $g_1(x)$ and $(1+x^{l_2})/(1+x^u)$ divides $g_2(v)$. Let

$$g(x) = \frac{1+x^u}{1+x^{l_2}} g_2(x) = \frac{1+x^u}{1+x^{l_1}} g_1(x),$$

then $g(x)$ is a polynomial. Evidently $G(U, g) \in \mathcal{S}$. We show that $G(u, g) = G(l_1, g_1) \cap G(l_2, g_2)$. Since $(l_1, l_2) = u$, $(1+x^{l_1}, 1+x^{l_2}) = 1+x^u$ and hence there exist $v_1(x)$ and $v_2(x)$ such that

$$(1+x^{l_1})v_1(x) + (1+x^{l_2})v_2(x) = 1+x^u.$$

It follows from this that

$$v_1(x)g_1(x) + v_2(x)g_2(x) = g(x)$$

Now multiply (9) by $v_1(x)$ and (10) by $v_2(x)$, and then add together, we obtain

$$(1+x^u)a(x) \equiv x^n g(x) \ (\mathrm{mod}(1+x^k)). \tag{14}$$

This implies that $G(l_1, g_1) \cap G(l_2, g_2) \subseteq G(u, g)$.

Conversely, if $a(x)$ is a solution of (14), then we have by multiplying (14) by $(1+x^{l_i})/(1+x^u)$,

$$(1+x^{l_i})a_i(x) \equiv x^u g_i(x) \,(\mathrm{mod}(1+x^k)), \quad i=1,2.$$

Hence, $G(u, g) \subset G(l_1, g_1) \cap G(l_2, g_2)$. Thus we have showed that $G(u, g) = G(l_1, g_1) \cap G(l_2, g_2)$. This completes the proof of Lemma 6. □

Corollary. *Let* $G(l_i, g_i) \in S$, $i=1,2$. *If* $G(l_1, g_1) \subseteq G(l_2, g_2)$ *then* $l_1 \mid l_2$ *and* $g_1(x) = (1+x^{l_1})g_2(x)/(1+x^{l_2})$ *or* $(1+x^{l_2})g_1(x) = (1+x^{l_1})g_2(x)$.

It is easily seen that if $G(l_1, g_1) \subseteq G(l_2, g_2)$ and $l_1 = l_2$ $(g_1 = g_2)$ then $g_1(x) = g_2(x)$ $(l_1 = l_2)$, hence $G(l_1, g_1) = G(l_2, g_2)$.

We have the following definitions:

Definition 1. Let $G(l_i, g_i) \in \mathcal{S}$, $i=1,2$ and $G(l_1, g_1) \subseteq G(l_2, g_2)$. We say that $G(l_1, g_1)$ is a predecessor of $G(l_2, g_2)$ and $G(l_2, g_2)$ is a successor of $G(l_1, g_1)$. If, furthermore, $l_2/l_1 = p_1 p_2 \cdots p_t$ is a product of t distinct primes, then we say that $G(l_1, g_1)$ is a t-predecessor of $G(l_2, g_2)$ and $G(l_2, g_2)$ is a t-successor of $G(l_1, g_1)$.

Definition 2. Let $\mathcal{F}$ be a subset of $\mathcal{S}$. We say that $\mathcal{F}$ has

Property A: if for any $G(l_0, g_0) \in \mathcal{F}$ and $G(l, g) \in \mathcal{S}$, $G(l, g) \subset G(l_0, g_0)$ implies $G(l, g) \in \mathcal{F}$.

We assume in Lemma 6′ to Lemma 10 below that $\mathcal{F}$ is a subset of S which has *Property* A.

Lemma 6′. *Let* $G(l_i, g_i) \in \mathcal{F}$ *and* $a_i \in G(l_i, g_i)$, $i=1,2$. *If* $a_1(x)$ *and* $a_2(x)$ *are cyclically equal, then* $a_1(x) = a_2(x)$. *In this case,* $G(l_1, g_1) \cap G(l_2, g_2) = G(u, g) \in \mathcal{F}$, *where* $u = (l_1, l_2)$ *and*

$$g(x) = \frac{1+x^u}{1+x^{l_1}} g_1(x) = \frac{1+x^u}{1+x^{l_2}} g_2(x).$$

Proof. Lemma 6′ is a modification of Lemma 6. The only thing that needs to be proved is that $G(u, g) \in \mathcal{F}$, but this is evident, since $\mathcal{F}$ has Property A. □

Lemma 7. *Let* $G(l_i, g_i) \in \mathcal{F}$ $(i=1,2)$ *and* $G(l_1, g_1) \subseteq G(l_2, g_2)$. *If* α *is a divisor of* l_2/l_1, *then* $G(\alpha l_1, h) \in \mathcal{F}$ *and* $G(l_1, g_1) \subseteq G(\alpha l_1, h) \subseteq G(l_2, g_2)$, *where* $h(x) = (1+x^{\alpha l_1})g_1(x)/(1+x^{l_1})$.

Proof. By the Corollary of Lemma 6, $g_1(x) = (1+x^{l_1})g_2(x)/(1+x^{l_2})$. Thus

$$h(x) = \frac{1+x^{\alpha l_1}}{1+x^{l_1}} g_1(x) = \frac{1+x^{\alpha l_1}}{1+x^{l_1}} \frac{1+x^{l_1}}{1+x^{l_2}} g_2(x) = \frac{1+x^{\alpha l_1}}{1+x^{l_2}} g_2(x)$$

is of degree $< m$. Evidently, $h(0) = 1$. Hence $G(\alpha l_1, h) \in \mathcal{F}$.

Let $b(x) \in G(\alpha l_1, h)$, i.e., $b(x)$ be a solution of the following congruence equation

$$(1+x^{\alpha l_1})b(x) \equiv x^n h(x) \,(\mathrm{mod}(1+x^k)). \tag{15}$$

Multiplying (15) by $(1+x^{l_2})/(1+x^{\alpha l_1})$, we obtain

$$(1+x^{l_2})b(x) \equiv x^n \frac{1+x^{l_2}}{1+x^{\alpha l_1}} h(x) \equiv x^n g(x) \,(\mathrm{mod}(1+x^k)),$$

which implies $G(\alpha l_1, h) \subseteq G(l_2, g_2)$. Hence $G(\alpha l_1, h) \in \mathcal{F}$. Similarly, $G(l_1, g_2) \subseteq G(\alpha l_1, h.)$ □

Lemma 8. *Let $G(l_0, g_0) \in \mathcal{S}$ and $G(l_i, g_i) \in \mathcal{F}$ $(i = 1, 2, \ldots, t)$ be t 1-predecessors of $G(l_0, g_0)$ in $\mathcal{F}$. If $\bigcap_{i=1}^t G(l_i, g_i) \neq \emptyset$, then $\bigcap_{i=1}^t G(l_i, g_i)$ is a t-predecessor of $G(l_0, g_0)$ in $\mathcal{F}$. Conversely, if $G(l, g)$ is a t-predecessor of $G(l_0, g_0)$ in $\mathcal{F}$, then there exist uniquely t 1-predecessors of $G(l_0, g_0)$ in $\mathcal{F}$ such that their intersection is $G(l, g)$.*

Proof. Since $G(l_i, g_i) \in \mathcal{F}$ are 1-predecessors of $G(l_0, g_0)$, $l_0/l_i = p_i$ are primes, $i = 1, \ldots, t$, and $p_i \neq p_j$ $(i \neq j)$. If $\bigcap_{i=1}^t G(l_i, g_i) \neq \emptyset$, we have by Lemma 6 that $\bigcap_{i=1}^t G(l_i, g_i) = G(l, g) \in \mathcal{F}$, where $l = (l_1, \ldots, l_t)$ and $g(x) = (1+x^l)g_i(x)/(1+x^{l_i})$ $(1 \leq i \leq t)$. It follows that $l_0/l = p_1 p_2 \cdots p_t$ is a product of t distinct primes and therefore $G(l, g)$ is a t-predecessor of $G(l_0, g_0)$ in $\mathcal{F}$. Conversely, if $G(l, g)$ is a t-predecessor of $G(l_0, g_0)$ in $\mathcal{F}$, then $l_0/l = p_1 \cdots p_t$, where $p_1, \ldots, p_t$ are distinct primes. Let $l_i = l_0/p_i$, $g_i(x) = (1+x^{l_i})g(x)/(1+x^l)$, $1 \leq i \leq t$. By Lemma 7, we have $G(l_i, g_i) \in \mathcal{F}$ and $G(l, g) \subseteq G(l_i, g_i) \subseteq G(l_0, g_0)$. We see that $G(l_i, g_i)$ are all 1-predecessors of $G(l_0, g_0)$ and uniquely determined by $G(l_0, g_0)$ and $G(l, g)$. Now repeatedly using Lemma 6, we obtain

$$\bigcap_{i=1}^t G(l_i, g_i) = G(l, g). \quad \square$$

For $G(l_0, g_0) \in \mathcal{F}$, we define $\mathcal{F}' = \{G(l, g) \in \mathcal{F} \mid G(l, g) \subset G(l_0, g_0)\}$ and denote $\mathcal{F}'_t$ the set of t-predecessors of $G(l_0, g_0)$ in $\mathcal{F}'$. We have

Lemma 9. $|\bigcup_{G \in \mathcal{F}'} G| = \sum_{t=1}^k (-1)^{t-1} \sum_{G \in \mathcal{F}'_t} |G|$. (*For the sake of simplicity, here and in the sequel, we often use G instead of $G(l, g)$.*)

Proof. At first, we prove that if $G(l, g) \subset G(l_0, g_0)$ and $G(l, g) \neq G(l_0, g_0)$, then $G(l, g)$ is contained in a 1-predecessor of $G(l_0, g_0)$. Since $G(l, g) \subset G(l_0, g_0)$ and $G(l, g) \neq G(l_0, g_0)$, we have $l \mid l_0$ and $l < l_0$. We may write $l_0/l = l'p$, where p is a prime and l' is a positive integer. Then by Lemma 7 we have $G(l, g) \subset G(l'l, h) \subset G(l_0, g_0)$, where $h(x) = (1+x^{l'})g(x)/(1+x^l)$. Evidently, $G(l'l, h)$ is a

1-predecessor of $G(l_0, g_0)$. Therefore we have

$$\bigcup_{G\in\mathscr{F}'} G = \bigcup_{G\in\mathscr{F}_1'} G.$$

Since $l_0 < k$, $|\mathscr{F}_1'| = s < k$. Using principle of inclusion and exclusion and Lemma 8, we obtain

$$\begin{aligned}\left|\bigcup_{G\in\mathscr{F}_1'} G\right| &= \sum_{G\in\mathscr{F}_1'} |G| - \sum_{\substack{G(l_i,g_i)\in\mathscr{F}_1' \\ i=1,2,\ l_1\neq l_2}} |G(l_1, g_1)\cap G(l_2, g_2)| + \cdots + (-1)^{s-1}\left|\bigcap_{G\in\mathscr{F}_1'} G\right| \\ &= \sum_{G\in\mathscr{F}_1'} |G| - \sum_{G\in\mathscr{F}_2'} |G| + \cdots + (-1)^{s-1} \sum_{G\in\mathscr{F}_s'} |G|.\end{aligned}$$

Note that $\mathscr{F}_t' = \emptyset$ for $t > s$. Lemma 9 follows immediately. □

Lemma 10. $|\bigcup_{G\in\mathscr{F}} G| = \sum_{t=0}^{k} (-1)^t \sum_{G\in\mathscr{F}} D_t^{\mathscr{F}}(G)\,|G|$, *where* $D_t^{\mathscr{F}}(G)$ *is the number of t-successors of G in* $\mathscr{F}$.

Proof. We use induction on $|\mathscr{F}|$. If $|\mathscr{F}| = 1$, the result is trivally true. Assume $|\mathscr{F}| > 1$. Choose a maximal element $G(l_0, g_0)$ in $\mathscr{F}$, $G(l_0, g_0) \in \mathscr{F}$ is maximal if for any $G(l, g) \in \mathscr{F}$, $G(l_0, g_0) \subseteq G(l, g)$ implies that $G(l_0, g_0) = G(l, g)$, hence $l_0 = l$ and $g_0(x) = g(x)$ and form $\bar{\mathscr{F}} = \mathscr{F} - \{G(l_0, g_0)\}$. It is clear that $\bar{\mathscr{F}}$ has Property A, since $G(l_0, g_0)$ is maximal. By induction hypothesis, we have

$$\left|\bigcup_{g\in\bar{\mathscr{F}}} G\right| = \sum_{t=0}^{k} (-1)^t \sum_{G\in\bar{\mathscr{F}}} D_t^{\bar{\mathscr{F}}}(G)\,|G|. \tag{16}$$

We distinguish two cases:

Case 1. $G(l_0, g_0) \cap (\bigcup_{G\in\bar{\mathscr{F}}} G) = \emptyset$. In this case, $G(l_0, g_0)$ is not a t-successor of any element in $\bar{\mathscr{F}}$ $(t \geq 1)$. Hence $D_t^{\bar{\mathscr{F}}}(G) = D_t^{\mathscr{F}}(G)$ for all $G(l, g) \in \bar{\mathscr{F}}$. Thus we have

$$\left|\bigcup_{G\in\mathscr{F}} G\right| = |G(l_0, g_0)| + \left|\bigcup_{G\in\bar{\mathscr{F}}} G\right| = \sum_{t=0}^{k} (-1)^t \sum_{G\in\mathscr{F}} D_t^{\mathscr{F}}(G)\,|G|,$$

which is the required result.

Case 2. $G(l_0, g_0) \cap (\bigcup_{G\in\bar{\mathscr{F}}} G) \neq \emptyset$. Let $\mathscr{F}'$ be the set of $G(l, g) \in \mathscr{F}$ satisfying $G(l, g) \subset G(l_0, g_0)$ and let $\mathscr{F}_t'$ be the set of t-predecessors of $G(l_0, g_0)$ in $\mathscr{F}'$. Then it is easily seen that

$$\bigcup_{G\in\mathscr{F}'} G = G(l_0, g_0) \cap \left(\bigcup_{G\in\bar{\mathscr{F}}} G\right).$$

Consequently

$$\left|\bigcup_{G\in\mathscr{F}'} G\right| = |G(l_0, g_0)| + \left|\bigcup_{G\in\bar{\mathscr{F}}} G\right| - \left|\bigcup_{G\in\mathscr{F}} G\right|. \tag{17}$$

Now suppose $G(l, g) \in \bar{\mathscr{F}}$ and $t \geq 1$. If $G(l, g) \in \mathscr{F}_t'$, then $G(l, g)$ has $G(l_0, g_0)$

as its t-successor, hence $D_t^{\bar{\mathcal{F}}}(G(l,g)) = D_t^{\mathcal{F}}(G(l,g)) - 1$, otherwise $D_t^{\bar{\mathcal{F}}}(G) = D_t^{\mathcal{F}}(G)$. We have also $D_t^{\mathcal{F}}(G(l_0, g_0)) = 0$ for $t \geqslant 1$. Thus

$$\sum_{G\in\bar{\mathcal{F}}} D_t^{\bar{\mathcal{F}}}(G)\,|G| = \sum_{G\in\mathcal{F}_t'} (D_t^{\mathcal{F}}(G) - 1)\,|G| + \sum_{G\in\bar{\mathcal{F}}-\mathcal{F}_t'} D_t^{\mathcal{F}}(G)\,|G|$$

$$= \sum_{G\in\mathcal{F}} D_t^{\mathcal{F}}(g)\,|G| - \sum_{G\in\mathcal{F}_t'} |G|,$$

and

$$\sum_{G\in\bar{\mathcal{F}}} D_0^{\bar{\mathcal{F}}}(G)\,|G| = \sum_{G\in\mathcal{F}} D_0^{\mathcal{F}}(G)\,|G| - |G(l_0, g_0)|.$$

By Lemma 9 and (16), we obtain

$$\left|\bigcup_{G\in\bar{\mathcal{F}}} G\right| = \sum_{t=0}^{k} (-1)^t \sum_{G\in\bar{\mathcal{F}}} D_t^{\bar{\mathcal{F}}}(G)\,|G|$$

$$= \sum_{G\in\mathcal{F}} D_0^{\mathcal{F}}(G)\,|G| - |G(l_0, g_0)| + \sum_{t=1}^{k} (-1)^t \sum_{G\in\mathcal{F}} D_t^{\mathcal{F}}(G)\,|G|$$

$$+ \sum_{t=1}^{k} (-1)^t \sum_{G\in\mathcal{F}_t'} |G|$$

$$= \sum_{t=0}^{k} (-1)^t \sum_{G\in\mathcal{F}} D_t^{\mathcal{F}}(G)\,|G| + \left|\bigcup_{G\in\mathcal{F}'} G\right| - |G(l_0, g_0)|. \tag{18}$$

Now Lemma 10 follows from (17) and (18). □

Now we proceed to prove Theorem 2. Since $\mathcal{S}$ obviously has Property A Lemmas 6–10 hold for $\mathcal{S}$. Lemma 6 states that if $a(x)$ and $b(x)$ are cyclically equal, then $a(x) = b(x)$. Hence $\overline{\beta(n,k)} = |\bigcup_{G\in\mathcal{S}} G|$. By Lemma 10, we have

$$\overline{\beta(n,k)} = \left|\bigcup_{G\in\mathcal{S}} G\right| = \sum_{t=0}^{k} (-1)^t \sum_{G\in\mathcal{S}} D_t^{\mathcal{S}}(G)\,|G|, \tag{19}$$

where $D_t^{\mathcal{S}}(G)$ is the number of t-successors of G in $\mathcal{S}$.

Before the proof of Theorem 2, we give a lemma which will simplify the proof.

Lemma 11. *Let $t \geqslant 1$. Let A_t be the set of positive integers which are products of t distinct primes and denote by $\pi_t(x)$ the number of positive integers in A_t which are less than x, where x is a real number. Then for any $G(l,g) \in \mathcal{S}$, we have*

$$D_t^{\mathcal{S}}(G(l,g)) = \pi_t\left(1 + \frac{m - d_l - j}{l}\right), \quad t \geqslant 1, \tag{20}$$

where $d_l = (k, l)$ and $j = \deg(g(x)) - d_l$. Furthermore, $\pi_t(1 + (m - d_l - j)/l) = 0$ if $j + l \geqslant m - 1$.

Proof. Let $G(l_1, g_1)$ be a t-successor of $G(l,g)$, $t \geqslant 1$. Then $G(l,g) < G(l_1, g_1)$ and l_1/l is a product of t distinct primes. Hence $\alpha = l_1/l \in A_t$. By Lemma 6, we

have $l_1 - l = \deg g_1(x) < m - d_l - j$. Therefore $2 \leqslant \alpha < (m - d_l - j)/l + 1$. Clearly distinct t-successors of $G(l, g)$ produce distinct α with $2 \leqslant \alpha \leqslant (m - d_l - j)/l + 1$. Hence

$$D_t^{\mathcal{G}}(G(l, g)) \leqslant \pi_t\left(1 + \frac{m - d_l - j}{l}\right). \tag{21}$$

On the other hand, if $\alpha \in A_t$ $(t \geqslant 1)$ satisfying $0 < \alpha < (m - d_l - j)/l + 1$, we have $\alpha \geqslant 2$.

Let $l_1 = \alpha l$, and $g_1(x) = (1 + x^{l_1})g(x)/(1 + x^l)$. Then $\deg g_1(x) < m$ and $G(l, g) \subset G(l_1, g_1)$. Hence $G(l_1, g_1)$ is a t-successor of $G(l, g)$. Note that distinct α produce distinct t-successors of $G(l, g)$, this yields

$$D_t^{\mathcal{G}}(G(l, g)) \geqslant \pi_t\left(1 + \frac{m - d_l - j}{l}\right). \tag{22}$$

Now (20) follows from (21) and (22).

Next we show that $\pi_t(1 + (m - d_l - j)/l) = 0$ if $j + l \geqslant m - 1$. By definition, we have $\pi_t(x) = 0$ if $x \leqslant 2$. Let $j + l \geqslant m - 1$, then $m - d_l - j + l = (m - d_l) - (j + l) + 2l \leqslant m - 1 - (m - 1) + 2l = 2l$, i.e., $m - d_l - j + l \leqslant 2l$. It follows immediately that $(m - d_l - j)/l + 1 \leqslant 2$, hence $\pi_t(1 + (m - d_l - j)/l) = 0$. This completes the proof. □

Proof of Theorem 2. We have shown that $D_t^{\mathcal{G}}(G(l, g)) = \pi_t(1 + (m - d_l - j)/l)$ and that $\pi_t(1 + (m - d_l - j)/l) = 0$ for $j + l \geqslant m - 1$. Hence we have

$$\sum_{G \in \mathcal{G}} D_t^{\mathcal{G}}(G)\,|G| = \sum_{l=1}^{m-2} \sum_{j=0}^{m-l-2} \sum_{g(x) \in P} \pi_t(1 + (m - d_l - j)/l)\,|G|,$$

where P is the set of polynomials $g(x)$ satisfying $\deg g(x) = j + d < m$, $g(0) = 1$, and $1 + x^{d_l}$ dividing $g(x)$. It is easily seen that the number of polynomials in P is $|P| = 2^{e_j}$, where $e_j = 0$ if $j = 0$, and $e_j = j - 1$ if $j > 0$. Since $G(l, g) = 2^{d_l}$, we obtain

$$\sum_{G \in \mathcal{G}} D_t^{\mathcal{G}}(G)\,|G| = \sum_{l=1}^{m-2} \sum_{j=0}^{m-l-2} \pi_t\left(1 + \frac{m - d_l - j}{l}\right) e^{d_l + e_j}. \tag{23}$$

Combine (19) and (23), we have

$$\begin{aligned}
\overline{\beta(n, k)} &= \left|\bigcup_{G \in \mathcal{G}} G\right| = \sum_{G \in \mathcal{G}} |G| + \sum_{t=1}^{k} (-1)^t \sum_{G \in \mathcal{G}} D_t^{\mathcal{G}}(G)\,|G| \\
&= 2^{m-2}\phi_{k,m-1} + \sum_{t=1}^{k} (-1)^t \sum_{l=1}^{m-2} \sum_{j=0}^{m-l-2} \pi_t\left(1 + \frac{m - d_l - j}{l}\right) e^{d_l + e_j} \\
&= 2^{m-2}\phi_{k,m-1} + \sum_{l=1}^{m-2} \sum_{j=0}^{m-l-2} \left[\sum_{t=1}^{k} (-1)^t \pi_t\left(1 + \frac{m - d_l - j}{l}\right)\right] e^{d_l + e_j}.
\end{aligned}$$

It is not difficult to see that

$$\sum_{t=1}^{k}(-1)^t\pi_t\left(1+\frac{m-d_l-j}{l}\right)=\sum_{2\leqslant q<1+(m-d_l-j)/l}\mu(q).$$

Hence

$$\overline{\beta(n,k)}=2^{m-2}\phi_{k,m-1}+\sum_{l=1}^{m-2}\sum_{j=0}^{m-l-2}\sum_{2\leqslant q<1+(m-d_l-j)/l}\mu(q)2^{d_l+e_j}.$$

And the result follows immediately from (1). □

5. The proof of Theorem 3

As an application of Theorem 2, we will prove in this section Bryant and Christensen's three conjectures (Theorem 3).

We compute, for $m=4$, 5, and 6, the values $\mu(q)2^{d_l+e_j}$, $(0\leqslant 1+j\leqslant m-2$ and $2\leqslant q(m-d_l-j)/l+1)$, in Tables 1–3, respectively.

Proof of Theorem 3. Note that for $m=4$, 5, 6, the triple summation in the formula of $\beta(n,k)$ in Theorem 2 is just the sums of values in Tables 1–3,

Table 1
Values of $\mu(q)2^{d_l+e_j}$ for $m=4$

		$\mu(q)2^{d_l+e_j}$	
l	j	$q=2$	$q=3$
1	0	-2	-2
2	0	$2(k,2)-4$	
1	1	-2	

Table 2
Values of $\mu(q)2^{d_l+e_j}$ for $m=5$

		$\mu(q)2^{d_l+e_j}$	
l	j	$q=2$	$q=3$
1	0	-2	-2
2	0	$-2(k,2)$	
3	0	$(k,3)-3$	
1	1	-2	-2
2	1	$2(k,2)-4$	
1	2	-4	

Table 3
Values of $\mu(q)2^{d_l+e_j}$ for $m=6$

		$\mu(q)2^{d_l+e_j}$		
l	j	$q=2$	$q=3$	$q=5$
1	0	-2	-2	-2
2	0	$-2(k,2)$	$2(k,2)-4$	
3	0	$(k,3)-3$		
4	0	$2(k,2)-4$		
1	1	-2	-2	
2	1	$-2(k,2)$		
3	1	$(k,3)-3$		
1	2	-4	-4	
2	2	$4(k,2)-8$		
1	3	-8		

respectively. Since Theorem 2 holds for $m = k - n \leqslant \frac{1}{4}k + 1$, we have

$$\beta(k-4, k) = \beta(k, k) - 4\phi_{k,3} - 2(k, 2) + 10, \quad \text{for } k \geqslant 12, \tag{24}$$

$$\beta(k-5, k) = \beta(k, k) - 8\phi_{k,4} - (k, 3) + 19, \quad \text{for } k \geqslant 16, \tag{25}$$

$$\beta(k-6, k) = \beta(k, k) - 16\phi_{k,5} - 4(k, 2) - 2(k, 3) + 48, \quad \text{for } k \geqslant 20. \tag{26}$$

Bryant and Christensen [2] verified that (24) hold for $k = 8$–11, (25) holds for $k = 11$–15, and (26) holds for $k = 15$–19. Thus (24)–(26) hold for $k \geqslant 8$, 11, and 15 respectively. This completes the proof. □

References

[1] N.G. de Bruijn, A combinatorial problem, Proc. K. Ned. Akad. Wet. Ser. A 49 (1946) 758–764.
[2] P.R. Bryant and J. Christensen, The enumeration of shift register sequences, J. Combin. Theory Ser. A 35 (1983) 154–172.
[3] P.R. Bryant and D. Everett, Cycles from feedback shift registers: a counting problem, in: Kyoto International Conference on Circuit and System Theory, Kyoto, Japan, 1970.
[4] J. Christensen and P.R. Bryant, On the number of cyclically distinct binary sequences having no internal periodicity and satisfying certain equality constraints, J. Combin. Theory Ser. B 20 (1976) 171–184.
[5] I.J. Good, Normal recurring decimals, J. London Math. Soc. 21 (1946) 169–172.